REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-19 are pending in the present application.

In the outstanding Office Action, Claims 1, 2, 4-8, and 10-19 were rejected under 35 U.S.C. §102(e) as anticipated by Chan (U.S. Patent No. 6,473,860); and Claims 3 and 9 were rejected under 35 U.S.C. §103(a) as unpatentable over Chan in view of Guthery (U.S. Patent No. 6,567,915).

In a non-limiting embodiment of the claimed invention, two separate communication paths of different types, the first and second communication paths, are set up as different channels on an identical transmission line or as different transmission lines. The first transmission path is used for communications other than the transfer of the executable programs and the second transmission path is used for transfer of the executable programs.[1]

In the non-limiting embodiment, the first communication path is an ordinary communication path between the program distribution device (server) and the client device. The second communication path is a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device.

Moreover, the non-limiting embodiment of the claimed invention encrypts an executable program to be distributed to the client device and executed within the tamper resistant processor by using the unique public key of the tamper resistant processor. The encrypted program is then transmitted from the program distribution device to the tamper

[1] Specification, page 9, lines 25-33.

resistant processor, which is the only entity that has the unique secret key corresponding to the unique public key. [2]

Turning now to the rejection of Claim 1 as anticipated by Chan, Applicants respectfully traverse the rejection because Chan fails to teach or suggest every element of Claim 1.

Claim 1 recites, *inter alia*,

> a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device;
>
> a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor, the first and second communication paths being set up as different channels on an identical transmission line or as different transmission lines;
>
> an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor; and
>
> a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

Indeed, Chan fails to teach or suggest these elements of Claim 1.

On the contrary, Chan only describes a system in which the central station 302 or 446 transmits the encrypted portions of the digital information to be distributed to the processing unit 310 or 410 through the communication link 318 or 448 while the clear (unencrypted)

[2] Specification, page 14, line 30 to page 15 lines 12.

portions of the same digital information are sent to the processing unit 310 or 410 through the communication lines 306 or 414.[3]

Chan clearly fails to teach or suggest utilizing a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device, specifically for the purpose of distributing executable programs to a type of the client device that has the tamper resistant processor provided inside.

Furthermore, Chan only describes a system in which the secure processor 314 or 420 decrypts the encrypted portions received from the central station 302 or 446, by using the decryption key received from the central station 302 or 446.[4]

Chan fails to teach or suggest any technique for encrypting an executable program by using the unique public key of the tamper resistant processor such that the encrypted program can be decrypted and executed only within the tamper resistant processor which is the only entity that has the unique secret key corresponding to the unique public key.

The combination of encrypting the program by using the public key of the tamper resistant processor and transmitting the encrypted program through the second communication path of a type as discussed above has the significant technical effect of ensuring that the encrypted program is directly delivered to the tamper resistant processor, which is the only entity that has the unique secret key corresponding to the unique public key.[5] Chan fails to teach or suggest a combination of such features for the purpose of realizing such a technical effect.

In view of the above-noted distinctions, Applicants respectfully submit that Claim 1 (and Claims 2-6) patentably distinguish over Chan. Claims 7, 13, and 14 are similar to Claim

[3] Chan, Fig. 1, Fig. 4, col. 3, lines 38-47 and 62-67, col. 4 lines 18-33, col. 7, lines 36-39 and 48-50, and col. 9, lines 35-40.
[4] Chan, col. 3, lines 57-59, col. 4, lines 27-36, col. 7, lines 51-53, and col. 10, lines 4-7.
[5] Specification, page 19, lines 6-14.

1. Applicants respectfully submit that Claims 7, 13, and 14 (and Claims 8-12, and 15-19) patentably distinguish over Chan for at least the reasons provided for Claim 1.

Consequently, in view of the above comments, it is respectfully submitted that the outstanding rejection is overcome and the pending claims are in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JW\203058US\203058US_AM 116.DOC

Surinder Sachar
Registration No. 34,423